UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/753,727	01/03/2001	Rosario Gennaro	RSW920000091US1	3760

7590 02/15/2006

Gerald R. Woods
IBM Corporation T81/503
P.O. Box 12195
Research Triangle Park, NC 27709

EXAMINER	
HENNING, MATTHEW T	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 02/15/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/753,727	**Applicant(s)** GENNARO, ROSARIO
	Examiner Matthew T. Henning	**Art Unit** 2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 November 2005*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,6,7,9-14,18,19,21-26,30,32,34-37,39,40,44 and 47-52* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,6,7,9-14,18,19,21-26,30,32,34-37,39,40,44 and 47-52* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *03 January 2001* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

This action is in response to the communication filed on 11/29/2005.

Response to Arguments

Applicant's arguments filed 11/29/2005 have been fully considered but they are not persuasive. Applicant argues primarily that:

a. Patel does not disclose a "C-bit exponent".

b. Patel disclosed outputting the lower $n-\omega(\log n)$ bits.

c. Section 5.1 of Patel discusses 's' which the examiner has pointed to as being a "short exponent" but in Section 5.1 's' actually only indicates that Patel is discussing "security" of his generator.

d. Section 5.1 was merely a proof of security section and not a Patel's algorithm.

e. Patel's generator is not secure, and therefore not enabled.

f. Patel uses a "perfect extender".

g. Patel selects the short exponent from the leading bits of a prior iteration.

The examiner notes the applicant's use of "result" to indicate the whole output of the bit generator, and the use of "output" to refer to the portion actually used by Patel as pseudo-random bits and will use the same terminology for consistency.

Regarding applicant's argument a., that Patel does not disclose a "C-bit exponent", the examiner does not find the argument persuasive. This is due to the following reason, as well as the responses to applicant's arguments b-g. Patel states on page 307 Section 2.1 Lines 1-2 that "*for efficiency purposes the exponent x is sometimes restricted to c bits (e.g. c=128 or 160 bits) since this requires fewer multiplications.*" Patel goes on to state in lines 1-3 of the following paragraph that "*we will also restrict x, in particular, we will restrict it to be slightly greater than O(log n) bits, but not to save on multiplications. The size of the exponent will be denoted ω(log n)*". Quite clearly, Patel disclosed that the exponent 'x' would be restricted to "c bits" denoted "ω(log n)". As such, the examiner does not find the argument persuasive. (Further see Patel Section 7.1).

Regarding applicant's argument b., that Patel disclosed outputting the lower n- ω(log n) bits, the examiner is unclear as to what this argument was meant to show considering that the argument does not reflect on the size of the exponent of Patel. However, the examiner agrees that in one embodiment, Patel disclosed outputting n - ω(log n) [or 'c'] pseudo-random bits. As such, the examiner does not find the argument persuasive.

Regarding applicant's argument c., that Section 5.1 of Patel discusses 's' which the examiner has pointed to as being a "short exponent" but in Section 5.1 's' actually only indicates that Patel is discussing "security" of his generator, the examiner does not find the argument persuasive. In section 5.1, 's' is a short exponent as can be seen in lines 12-14 of section 5.1. Therefore, the examiner does not find the argument persuasive.

With regards to applicant's argument d., that section 5.1 was merely a proof of security section and not part of the algorithm, the examiner has considered the argument and does not find the argument persuasive. See MPEP Section 2122

> ***UTILITY NEED NOT BE DISCLOSED IN REFERENCE***
>
> *In order to constitute anticipatory prior art, a reference must identically disclose the claimed compound, but no utility need be disclosed by the reference. In re Schoenwald, 964 F.2d 1122, 22 USPQ2d 1671 (Fed. Cir. 1992) (The application claimed compounds used in ophthalmic compositions to treat dry eye syndrome. The examiner found a printed publication which disclosed the claimed compound but did not disclose a use for the compound. The court found that the claim was anticipated since the compound and a process of making it was taught by the reference. The court explained that "no utility need be disclosed for a reference to be anticipatory of a claim to an*

old compound." 964 F.2d at 1124, 22 USPQ2d at 1673. It is enough that the claimed compound is taught by the reference.).

As such, simply because section 5.1 deals with proving the security of the system, does not mean that the section is irrelevant. Section 5.1, is a section proving the security of the algorithm of section 5. As recited on page 16 Lines 13-18, Patel disclosed using short exponents as the exponents for the system. Further, as discussed above with regards to argument a., Patel clearly disclosed limiting the exponent to a short exponent (See Patel Section 7.1). As such, the examiner does not find the argument persuasive.

Regarding applicant's argument e, that the generator of Patel utilizing short exponents, as shown in section 7.1 of Patel, is not secure, and therefore is not enabled, the examiner does not find the argument persuasive. Whether the generator is secure or not is a moot point as the generator described in Patel meets the limitations of the claim language. Further, Patel does enable one of ordinary skill in the art to make and use the generator with short exponents as has been claimed in the present application. The security of such a system is irrelevant to the enablement of the reference. However, for arguments sake, if Patel was not enabling for making the claimed invention, then the claims themselves must not be enabled as well, since Patel reads on the claims. Therefore, the examiner does not find the argument persuasive.

Regarding applicant's arguments f and g, the examiner does not find the argument persuasive. There are no limitations in the claims which prohibit the use of the leading bits as the short exponent or the use of a perfect extender. Therefore, the examiner does not find the arguments persuasive.

Because the arguments have not been found persuasive, the examiner is maintaining the prior art rejections in view of Patel as set forth below.

DETAILED ACTION

All rejections and objections not set forth below have been withdrawn.

Claims 1-2, 6-7, 9-14, 18-19, 21-26, 30, 32, 34-37, 39-40, 44, and 47-52 have been examined.

Claims 3-5, 8, 15-17, 20, 27-29, 31, 33, 38, 41-43, and 45-46 have been cancelled.

Specification

The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: The specification fails to provide antecedent basis for the claim terminology of setting "(N-C) uppermost contiguous ones of the bits" to zero and C lowermost contiguous ones of bits are random. See the rejection of claim 52 under 35 USC 112 1st paragraph below.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claim 52 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Although the specification provides antecedent basis for the limitation of setting the top (N-C) bits to zero and leaving the other bits random, the specification does not provide antecedent basis for setting (N-C) uppermost **contiguous ones of bits** to zero and leaving the lowermost **contiguous ones of bits** random. As a result, one of ordinary skill in the art would not have been able to determine that the applicant was in possession of the claimed invention. Therefore, claim 52 is rejected for failing to meet the description requirement of 35 USC 112 1st paragraph.

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 52 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The term "effectively-short" in claim 52 is a relative term which renders the claim indefinite. The term "effectively-short" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. One of ordinary skill in the art would not be able to determine how “short” the exponent would need to be in order to be classified as “effectively-short”. Therefore, claim 52 is rejected for failing to particularly point out and distinctly claim the subject matter which the applicant regards as the invention.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 13-14, 18-19, 21-22, 24-26, 30, 32, 34-35, 37, 39-40, 44, 47, and 49-52 are rejected under 35 U.S.C. 102(b) as being anticipated by Patel et al ("An Efficient Discrete Log Pseudo Random Generator") hereinafter referred to as Patel.

Regarding claim 13, Patel disclosed a system for efficiently generating pseudo-random bits in a computing environment, comprising: means for providing an input value comprising C random bits (See Patel Page 313 Section 5 Line 10 and section 7.1 s_i wherein C = ω(log n)); means for generating an output sequence comprising N pseudo-random bits (See Patel Page 313 Section 5 Lines 11-12 and section 7.1 x_{i+1}) using the provided C-bit input value as a short exponent x of a 1-way function G**x mod p that comprises modular exponentiation modulo a safe N-bit prime number P (See Patel Page 313 Section 5 Line 10 wherein the function $x_{i+1} = g^{x_i}$ mod p is one-way, Section 7.1 s as the short exponent, and Page 307 Paragraph 6 Lines 7-8) wherein a base G of the modular exponentiation is a fixed generator value (See Patel Page 304 Section 1 Lines 3-4), means for separating the N bits of the generated N-bit output sequence into a C-bit portion and an (N-C)-bit portion (See Patel Section 7.1 wherein the output of the generator are the trailing n - ω(log n) bits of x_i and s_i is the leading ω(log n) bits of x_i); and means for using the C-bit portion of the generated N-bit output sequence as the provided input value for the next iteration of the means for generating (See Patel Section 7.1) while using the (N-C)-bit portion of the generated N-bit output sequence as pseudo-random output bits (See Patel Section 7.1), until a desired number of pseudo-random output bits have been generated (See Patel section 5 Lines 9-11, wherein the feedback is performed for all i>0).

Regarding claim 25, Patel disclosed a programmatic method for efficiently generating pseudo-random bits, comprising the steps of: providing an input value comprising C random bits (See Patel Page 313 Section 5 Line 10 and section 7.1 s_i wherein C = ω(log n)); generating an output sequence comprising N pseudo-random bits (See Patel Page 313 Section 5 Lines 11-12 and section 7.1 x_{i+1}) using the provided C-bit input value as a short exponent x of a 1-way function G**x mod p that comprises modular exponentiation modulo a safe N-bit prime number P (See Patel Page 313 Section 5 Line 10 wherein the function $x_{i+1} = g^{x_i}$ mod p is one-way, Section 7.1 s as the short exponent, and Page 307 Paragraph 6 Lines 7-8) wherein a base G of the modular exponentiation is a fixed generator value (See Patel Page 304 Section 1 Lines 3-4); separating the N bits of the generated N-bit output sequence into a C-bit portion and an (N-C)-bit portion (See Patel Section 7.1 wherein the output of the generator are the trailing n - ω(log n) bits of x_i and s_i is the leading ω(log n) bits of x_i); and using the C-bit portion of the generated N-bit output sequence as the provided input value for the next iteration of the means for generating (See Patel Section 7.1) while using the (N-C)-bit portion of the generated N-bit output sequence as pseudo-random output bits (See Patel Section 7.1), until a desired number of pseudo-random output bits have been generated (See Patel section 5 Lines 9-11, wherein the feedback is performed for all i>0).

Regarding claim 39, Patel disclosed an encryption system, comprising: means for providing an input value comprising: C random bits (See Patel Page 313 Section 5 Line 10 and section 7.1 s_i wherein C = ω(log n)); means for generating an output sequence comprising N pseudo-random bits (See Patel Page 313 Section 5 Lines 11-12 and section 7.1 x_{i+1}) using the provided C-bit input value as a short exponent x of a 1-way function G**x mod p that comprises modular exponentiation modulo a safe N-bit prime number P (See Patel Page 313 Section 5 Line 10 wherein the function $x_{i+1} = g^{x_i}$ mod p is one-way, Section 7.1 s as the short exponent, and Page 307 Paragraph 6 Lines 7-8) wherein a base G of the modular exponentiation is a fixed generator value (See Patel Page 304 Section 1 Lines 3-4), means for separating the N bits of the generated N-bit output sequence into a C-bit portion and an (N-C)-bit portion (See Patel Section 7.1 wherein the output of the generator are the trailing n - $\omega(\log n)$ bits of x_i and s_i is the leading $\omega(\log n)$ bits of x_i); and means for using the C-bit portion of the generated N-bit output sequence as the provided input value for the next iteration of the means for generating (See Patel Section 7.1) while using the (N-C)-bit portion of the generated N-bit output sequence as pseudo-random output bits (See Patel Section 7.1), until a desired number of pseudo-random output bits have been generated (See Patel section 5 Lines 9-11, wherein the feedback is performed for all i>0); and means for using the desired number of generated pseudo-random bits as input to an encryption operation (See Patel Page 305 Lines 15-17).

Regarding claims 14, 26, and 40, Patel disclosed that the 1-way function is based upon an assumption known as “the discrete logarithm with short exponent" assumption (See Patel Page 307 Section 2.1).

Regarding claims 18, 30, and 44, Patel disclosed that the C=160 (See Patel Section 2.1 Lines 1-2 wherein x is the input of 160 bits) and N=1024 (See Patel Page 307 Lines 5-6) (Further see the abstract).

Regarding claims 19, and 32, Patel disclosed that the C is at least 160 bits (See Patel Section 2.1 Lines 1-2 wherein x is the input of 160 bits) and N is at least 1024 bits (See Patel

Abstract Lines 11-13 wherein n is the number of bits output by the generator prior to bit extraction as disclosed by Patel in Section 6) (Further See Section 7.1).

Regarding claims 21, 34, and 47, Patel disclosed that the (N-C)-bit portion is concatenated to pseudo-random output bits previously generated by the means for generating (See Patel Abstract and Section 7.1).

Regarding claims 22, and 35, Patel disclosed that the (N–C)-bit portion is selected from the N bits of the generated output sequence as a contiguous group of bits (See Patel Section 7.1 Lines 3-4).

Regarding claims 24, and 37, Patel disclosed means for using the desired number of generated pseudo-random output bits as input to an encryption operation (See Patel Page 305 Lines 15-17).

Regarding claims 49, 50, and 51, Patel disclosed that N is greater than or equal to (C*6) (See Patel Abstract wherein C=128 and n=1024).

Regarding claim 52, Patel disclosed a programmatic method for efficiently generating pseudo-random bits, comprising the steps of: providing an N-bit input value in which (N-C) uppermost contiguous ones of the bits are all set to zeros and in which C lowermost contiguous ones of the bits are random (See Patel Page 313 Lines 22-27); generating an output sequence comprising N pseudo-random bits using the provided N-bit input value as an effectively-short, C-bit exponent x of a 1-way function G**x mod P that comprises modular exponentiation modulo a safe N-bit prime number P, wherein a base G of the modular exponentiation is a fixed generator value (See Patel Page 313 Section 5 Line 10 wherein the function $x_{i+1} = g^{x_i}$ mod p is one-way, Section 7.1 s as the short exponent, Page 304 Section 1 Lines 3-4, Page 307 Paragraph

6 Lines 7-8, and Page 313 Lines 22-27); separating the N bits of the generated N-bit output sequence into a C-bit portion and an (N-C)-bit portion (See Patel Section 7.1 wherein the output of the generator are the trailing n - ω(log n) bits of x_i and s_i is the leading ω(log n) bits of x_i); creating a new N-bit input value in which the (N-C) uppermost contiguous ones of the bits are all set to zeros and in which the lowermost C contiguous ones of the bits are set to the C-bit portion (See Patel Section 7.1 and Page 313 Lines 22-27); and using the new N-bit input value as the provided input value for a next iteration of the generation step while using the (N-C)-bit portion of the generated N-bit output sequence as pseudo-random output bits, until a desired number of pseudo-random output bits have been generated (See Patel Section 7.1).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> *A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.*

Claims 1-2, 6-7, 9-12, 23, 36, and 48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Patel as applied to claims 13 and 25 respectively above, and further in view of Schneier ("Applied Cryptography").

Patel disclosed Regarding claims 13, 23, and 36, Patel disclosed a system for efficiently generating pseudo-random bits in a computing environment, comprising: means for providing an input value comprising C random bits; means for generating an output sequence comprising N pseudo-random bits using the provided C-bit input value as a short exponent x of a 1-way function G**x mod p that comprises modular exponentiation modulo a safe N-bit prime number P wherein a base G of the modular exponentiation is a fixed generator value, means for separating the N bits of the generated N-bit output sequence into a C-bit portion and an (N-C)-bit portion; and means for using the C-bit portion of the generated N-bit output sequence as the provided input value for the next iteration of the means for generating while using the (N-C)-bit portion of the generated N-bit output sequence as pseudo-random output bits, until a desired number of pseudo-random output bits have been generated (See rejection of claim 13 above), but Patel failed to disclose that this system was implemented in software, and further failed to disclose that the input comprised non-contiguous bits of the previous output. However, Patel did disclose that these pseudo-random bits were for encryption (See Patel Page 305 Lines 15-17).

Schneier teaches that any encryption algorithm can be implemented in software and that doing so helps with flexibility and portability, ease of use, and ease of upgrade (See Schneier Page 225 Paragraph 7 Lines 1-3). Schneier further teaches that software encryption programs are popular (See Schneier Page 225 Paragraph 8 Line 1). Schneier also teaches that in order to reach a maximal period for a pseudo-random bit generator, the feedback bits should be a primitive polynomial mod 2 (See Schneier Page 374 lines 9-20, and further shows an example of this type of feedback (See Schneier Page 375 Figure 16.4).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Schneier to the pseudo-random bit generator of Patel, by implementing the generator in software, and by providing primitive polynomial mod 2 feedback to the generator. This would have been obvious because the ordinary person skilled in the art would have been motivated to improve the portability, ease of use, and ease of upgrade of the generator, and to provide the longest period for the generator to ensure the most produced bits before cycling.

Claims 2, 6-7, 9-10, 12 and 48 are rejected for the same reasons as claim 14, 18-19, 21-22, 24, and 49 above, as applied to claim 1.

Conclusion

Claims 1-2, 6-7, 9-14, 18-19, 21-26, 30, 32, 34-37, 39-40, 44, and 47-52 have been rejected.

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew T. Henning whose telephone number is (571) 272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Matthew Henning
Assistant Examiner
Art Unit 2131
2/7/2006

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100